

## **DETAILED ACTION**

### **Continued Examination Under 37 CFR 1.114**

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/09/2011 has been entered.

### **Response to Arguments**

2. Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

### **Claim Rejections - 35 USC § 103**

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 3, 5, 7-8, 9, and 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sakaki et al. (US-5826007), and further in view of Sourgen (US-5101121).

a. Referring to claims 1, 9 and 11:

Regarding claims 1, 9 and 11, Sakaki teaches a chip comprising: a microprocessor; and an integrated non-volatile programmable memory that stores protection data in a protection data memory portion and protected data in a protected data memory portion (Col 4, Line 13-48..... chip comprising CPU, NV-RAM storing protected test memory (storing a test program) and

protection bits (S1, S2) for protecting access to the protected memory), wherein said protection data defines a protection level for authorizing or denying access to said protected data memory portion by said microprocessor while a program is executed (Col 4, Line 42 thru Col 5, Line 48.... The protection bits (s1, S2) define a protection level for the protected data in that access (Read/write) to the data is authorized when the bits are in their low level (logic 0) and denied when s1 is changed to a high level (logic 1)), and wherein said protection data is modifiable only to increase said protection level by non-reversibly reducing access to a part of the protected data memory portion (Col 5, Line 13-62.... protection bit s2 is modified to high level (logic 1) after shipment to increase the protection level from the initial state and deny access to the stored test program), and said protected data includes data to activate or deactivate an optional feature of the chip (Col 4, Line 28-30 and Col 5, Line 34-42.... protected test program used to enable/disable read/write (input/output) to the NV memory from an external terminal).

Sakaki teaches the protection bit to increase the protection level by restricting access to the protected data. Sakaki does not teach non-reversibly restricting access using the protection bit (i.e. a situation where access to the protected data is not possible again). However, such non-reversible protection of data (using protection/lock bits) stored on a chip is well known in the art and used by chip manufacturers after a final test on the chip to non-reversibly disable access to the protected test data. For instance, Sourgen teaches non-reversible security/protection bits for integrated circuit chip wherein a first bit is used to non-reversibly lock a test data portion (pertaining to the manufacturer) before the chip is shipped to a customer at which a second bit can be used to further non-reversibly lock another protected data portion (pertaining to the customer) of the chip (See Sourgen, Col 6, Line 49-68). Therefore, one of ordinary skill would

have been motivated to modify the protection bits of Sakaki as taught by Sourgen to non-reversibly protect the protected data portion of the chip by permanently reducing access to the protected data for the purpose of increasing the security of the data on the chip against tampering and malicious access.

a. Referring to claim 3:

Regarding claim 3, the combination of Sakaki and Sourgen teaches a chip according to Claim 1, wherein said protection data includes a password, said access being authorized/denied through a password check (Col 5, Line 13 thru Col 6, Line 12.... s1 and s2 protection bits with s2 comprising the password check. If s1=1, the chip is password-protected and access to the protected data is denied. If s1=1 and s2=1 (s2 being the password check), a manufacturer can then access the protected data after shipment).

a. Referring to claim 5:

Regarding claim 5, the combination of Sakaki and Sourgen teaches a chip according to Claim 1, wherein said optional feature is a connection to an external device for downloading a program and/or data from said external device (Col 5, Line 34-43.... connection to an external terminal for inputting or outputting data into the memory of the chip).

a. Referring to claim 7:

Regarding claim 7, the combination of Sakaki and Sourgen teaches a chip according to Claim 1, wherein said protection data includes at least one address value defining an address limit from which the data stored at said memory are protected data and access to such protected data is denied (See the response to argument and Col 6, Line 3-16 and Col 6, Line 5-14.... based

on the value of the s1, s2 protection bits, the bus control logic defines the address of the protected data (test program) which the CPU can execute).

a. Referring to claim 8:

Regarding claim 8, the combination of Sakaki and Sourgen teaches a chip according to Claim 7, wherein said protected data include includes programs and data operating a conditional-access dedicated microprocessor (Col 4, Line 13-35.... protected memory storing system program and fixed data for operating a microprocessor) .

a. Referring to claim 12:

Regarding claim 12, the combination of Sakaki and Sourgen teaches a chip according to Claim 1 further comprising a random logic coupled between said integrated non-volatile programmable memory and a connection bus of said microprocessor (Fig 2. bus line control circuit coupled between the protected memory and the processor).

**5. Claim 6 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sakaki et al. (US-5826007) and Sourgen (US-5101121), and further in view of Madter et al. (US-20050033951).**

a. Referring to claim 6:

Regarding claim 6, the combination of Sakaki and Sourgen teaches the protected data includes data to activate/deactivate and external feature of the microprocessor such as write/read to an external terminal. Sakaki does not teach external feature of downloading a boot program from an external memory. However, the concept of protecting a chip from downloading an external boot program (which might be malicious) using protection bits is well known in the art. For instance, Madter discloses an on-chip security method wherein a security value (protection

data) is used to protect flash memory. The password is used to protect access to instructions for downloading an external boot program to be run by the chip. When a password is received (password check), download of the external boot program is inhibited (See Sakaki, Para 32-35). Therefore, it would have been obvious to modify Sakaki's protection system to include protection against downloaded boot programs wherein the protection bits of Sakaki are used to enable or disable access to external boot programs for the purpose of securing the chip from both unauthorized and malicious access.

a. Referring to claim 10:

Regarding claim 10, Sakaki teaches a device as claimed in Claim 9, wherein the device is intended to process encrypted video/audio data (See Madter, Para 3... PDA and mobile devices for processing encrypted video/audio as known in the art).

**6. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sakaki et al. (US-5826007) and Sourgen (US-5101121), and further in view of Boyle et al. (US-6118870).**

a. Referring to claim 13:

Regarding claim 13, the combination of Sakaki and Sourgen teaches a chip according to claim 1. Sakaki does not explicitly teach the chip having a MIPS instruction set. However, Boyle teaches a chip having a MIPS instruction set (See Boyle, Col 10, Line 3-18). Therefore it would have been obvious to one of ordinary skill to implement Sakaki's chip as a microprocessor having a MIPS instruction set for the benefit of utilizing RISC architecture which provides higher performance by making instruction execute quickly and is designed for use with high level programming languages.

**7. Claims 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sakaki et al. (US-5826007) and Sourgen (US-5101121), and further in view of Moller et al. (US-20030014653).**

a. Referring to claim 14:

Regarding claim 14, the combination of Sakaki and Sourgen teaches the method of claim 11 wherein the protected data is a test program defined by an address range which is protected by protection data (bits) which is modifiable to increase the protection by denying access to the test program. Sakaki does not teach the chip protecting a stored conditional access program (such as encryption/decryption program for content) using the mechanism for protecting the test program. However, storing and protecting conditional access programs (such as encryption/decryption program for content) on a chip is well known in the art. For instance, Moller discloses a method of storing a conditional access programs (such as encryption/decryption program for content) on a chip and protecting access to the program using protection bits (See Moller, Para 6-8). Therefore, one of ordinary skill would have been motivated to modify Sakaki's teaching to store a conditional access program on the chip and to protect access to the program using the same mechanism used to protect the test program. This is advantageous in the art of media and content distribution wherein the decryption key program is stored on the chip of an STB or media player and protected from unauthorized users using the protection bits (i.e. if a correct password is not received, the protection bits are modified to restrict access to the decryption program).

a. Referring to claim 15:

Regarding claim 15, the combination of Sakaki, Madter and Moller teaches the method of claim 14 wherein the access to the part of the first protected data memory portion is non-

reversibly reduced by modification of the first set of address data (See the rejection in claims 7 and 14).

a. Referring to claim 16:

Regarding claim 17, the combination of Sakaki, Madter and Moller teaches the method of claim 15 further comprising: using at least a second authorized access to modify a second protected data portion in the first integrated non-volatile memory, wherein the second protected data portion comprises a set of conditional access microprocessor data and a deciphering key, with the deciphering key allocated to a lowest address of the second protected data portion; protecting the access to the second protected data portion in the first integrated non-volatile memory by modifying a second protection data portion of the first integrated non-volatile memory in order to deny access to the second protected data portion, wherein said second protection data portion is modifiable only to increase said protection level by non-reversibly reducing access to at least a part of the second protected data memory portion (See the rejection in claims 1, 14 and 15).

a. Referring to claim 17:

Regarding claim 17, the combination of Sakaki, Madter and Moller teaches the method of claim 16 wherein the second protection data portion comprises a second address data that is the lowest address in the second protected data portion readable by the microprocessor, wherein the set of address data is initially associated with the lowest address of the second protected data portion; and wherein the second protection data portion is modifiable only to increase said protection level by increasing the value of the second address data (See the rejections in claims 1, 14 and 15).

### **Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571) 270-3854. The examiner can normally be reached on Monday - Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 270-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/536,732  
Art Unit: 2432

Page 10

/IZUNNA OKEKE/  
Examiner, Art Unit 2432

/Minh Dinh/  
Primary Examiner, Art Unit 2432